USAWC STRATEGY RESEARCH PROJECT

AIRLINE SECURITY AND A STRATEGY FOR CHANGE

by

Colonel Timothy J. Welch
United States Army Reserve

Colonel Slim Connors
Project Adviser

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
15 MAR 2006		**00-00-2005 to 00-00-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Airline Security and a Strategy for Change	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Timothy Welch	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**22**	

ABSTRACT

AUTHOR: Colonel Timothy J. Welch

TITLE: Airline Security and a Strategy for Change

FORMAT: Strategy Research Project

DATE: 15 January 2006 WORD COUNT: 5938 PAGES: 21

KEY TERMS: Biometrics, Federal Flight Deck Officer, Positive Passenger Bag Match, Airline Security

CLASSIFICATION: Unclassified

On September 11, 2001, the United States of America, a free and open society with numerous points of vulnerability, found itself at war against a coordinated terrorist threat. Obligated to secure the Homeland, the United States Government scrambled to develop measures that would uphold societal values while providing an in-depth defense capable of ensuring a more secure society. By executive order, agencies were created to protect the Homeland. The full effectiveness and efficiency of those newly created agencies and processes remains in question. Some will argue that they are fully effective while others emphatically proclaim them a complete failure. This paper uses U.S. airline security as a basis for analyzing the bureaucratic organizations created to deal with the terrorist threat. It begins with a review of airlines' security on 9/11. The main discussion describes and explains the actions taken subsequent to 9/11, including an evaluation of the strengths and identification of the weaknesses and flaws. The paper concludes with a recommended strategy that would, if implemented, provide a more secure U.S. airline industry.

AIRLINE SECURITY AND A STRATEGY FOR CHANGE

At 0545 on the morning of September 11, 2001, most Americans slept, unaware of the disastrous plan being executed. Seemingly secure in a nation that cherished freedom, openness, great cities, and modern transportation, few would have imagined the plot beginning to unfold in the northeastern Unites States. Driven by hatred of the very things Americans value most, foreign terrorists launched a plan designed to exploit the vulnerabilities of an open society. Terrorists, under the leadership of Osama Bin Laden, boarded aircraft in Boston, Massachusetts, Newark, New Jersey, and Washington, DC on a mission that would kill thousands of Americans, and as a result, make Homeland defense the nation's number one priority. Al Qaeda, a Middle Eastern terrorist network that spans the globe and is supported by various rogue nations, was unsuccessful in a previous attempt at destroying the World Trade Center. This time however, trained pilots were given the mission of flying commercial airliners into the World Trade Center, the Pentagon, and either the White House or Capitol Building in Washington, DC. Their plan was brilliant insofar as the victim (the American people) actually supplied the means (American owned aircraft, used as missiles) to those executing that criminal and highly destructive act. Such a plan was made possible by the American insistence on a free and open society. Who in this nation imagined that enemy agents would take advantage of what had never before been considered an area of vulnerability to send their message of hatred? It is no coincidence, and certainly highly symbolic, that the terrorists chose planes operated by the carriers United and American to fly into three of the United States' symbols of strength and prosperity. Had their goal been to inflict mass destruction and devastation to the country, as opposed to sending a message announcing their intense hatred of America's free society, these terrorists might have chosen targets such as Three Mile Island (and/or other nuclear reactor facilities) along with Red Stone or Pine Bluff Arsenals. These targets might have provided literally "more bang for the buck."

The nation learned a terrible lesson that day. The very things that Americans cherish make the country vulnerable to terrorism of catastrophic proportions. The threat of mass-destruction became a Homeland issue. Obligated to secure the Homeland, the United States Government scrambled to develop measures that would uphold societal values while providing an in-depth defense and a more secure society. By executive order, agencies were created to protect the Homeland.[1] The full effectiveness and efficiency of those newly created agencies and systems remains in question. Some will argue that they are fully effective, while others emphatically proclaim them a complete failure.[2] Securing the airline industry is of national

importance. Multiple threats directed at this vital yet extremely vulnerable sector of the United States economy deem this an issue of national concern. This paper discusses why and how airline security must be changed, evaluates the variety of systems employed subsequent to 9/11, then offers a recommended strategy which could provide both an improved security posture and the peace of mind demanded by travelers.

The hijacking of commercial airliners is not a new phenomenon. During the 1960s and 1970s, there were many incidents in the United States and around the world in which aircraft were commandeered.[3] These events involved individuals using hijacking as a technique to extort large sums of money. The hijackers were usually religious or political fanatics seeking the limelight and money by taking an airliner to Cuba and then holding airline crew and passengers hostage. The concern by people close to the industry that the publicity to be gained by the destructive use of a jetliner was attractive to those seeking political or terrorist gains was no secret. Since the 1970s there have been nine hijacking events involving U.S. carriers or flights arriving or departing the United States where at least one passenger was killed.[4] Although the number of such incidents might seem insignificant, concern began to grow about the safety of passengers and the possibility for more destructive use of airliners for political or terrorist purposes. It was a different time and the threat did not, in any way, approach what it is today. The horrific events of September 11, 2001, validated those previously minor fears and brought about the need for a radically new approach to securing an industry so vital to the national economy. The current threat must serve as the impetus for change in how the air transport system is secured.

Biometric scanning represents a radical departure from current methods. Biometric systems consist of hardware and software used to capture various human characteristics, compare them to information contained in a database, then decide if enough criteria has been met to positively verify identification. Thanks to recent technological advancements, the use of biometric scanning, in conjunction with security methods already in place, would offer a level of screening that would profoundly increase security.

> Together we will confront the threat of terrorism. We will take strong precautions aimed at preventing terrorists' attacks and prepare to respond effectively if they come again. We will defend our country; and while we do so we will not sacrifice the freedoms that make our land unique.
>
> —President George W. Bush, October 8, 2001.[5]

Within minutes of the deviation of United Airlines flights 175 and 93, and American Airlines flights 11 and 77 from their cleared routes, the governments of both the United States and

Canada reacted by closing down their air transport systems. More than 200 flights inbound to the United States were diverted to Canadian airports.[6] For the first time in history, airports from coast to coast grew quiet with hundreds of planes, carrying thousands of passengers, forced to land immediately, stranding travelers all over the United States and overseas. During those critical first moments it became clear to strategic leaders that the freedom with which air travel had always been conducted was a thing of the past.

An analysis of the loss of four aircraft, from two different airlines, to terrorists made it clear that more effective techniques for screening passengers and crewmembers were needed. The creation and implementation of new techniques became a joint responsibility of the government and the commercial airlines, both passenger and cargo carriers.[7] The government responded by creating the Office of Homeland Security on October 8, 2001.[8] The Strategic objectives of Homeland Security, in order of priority, are to:

- Prevent terrorist attacks in the United States
- Reduce America's vulnerability to terrorism
- Minimize the damage and swiftly recover from attacks that do occur.[9]

These objectives were to be accomplished by using increased intelligence surveillance combined with active pursuit of terrorists, both domestically and abroad. On November 19th, 2001, the Transportation Security Administration (TSA) was created as part of the Aviation Security Act.[10] Originally organized as a subcomponent of the United States Department of Transportation, the TSA was charged with developing safety procedures and creating policies to ensure the safety of U.S. air traffic and other forms of transportation. Responsibility for administration of the TSA was subsequently moved, in 2003, to the Department of Homeland Security.[11] Domestic and flag carriers responded by emplacing new screening criteria for all flights, both domestic and international. Anyone having aircraft access became subject to constant verification and physical searches (only flight crewmembers were exempt from random personal searches). All aircraft were required to have interior security inspections prior to the boarding of passengers. The power of Captains was reemphasized by airlines, who gave them full authority to evaluate the security of their aircraft and take appropriate action prior to departure.

Immediate Changes

During the months immediately after the attacks, a series of sweeping changes were made that significantly increased airline security. The FAA increased the size of the Federal Air Marshal program, cockpit doors were strengthened and further fortified with electronic locking

devices, and serious consideration was given to a Federal Flight Deck Officer (FFDO) Program that would allow crewmembers to carry weapons.[12] Most importantly though, emphasis was placed on long-term solutions in which the advice of, and input from, crewmembers would be incorporated. Some of the recommendations were the transfer of aviation security oversight to a law enforcement agency, a complete overhaul of the U.S. security screening checkpoint system, the fielding of a screening system capable of detecting weapons and explosive devices, making use of available technology to positively identify all personnel entering secure airport areas, expanding the Positive Passenger Bag Match criteria, and gathering information on passengers about special capabilities they might have for use by Captains in an emergency.[13] In the years since 9/11, most of these immediate recommendations have been used. Efforts are now focused on implementing more effective long-term solutions. One of the more successful programs implemented is the Federal Flight Deck Officer program. Pilots who meet strict qualifications are allowed to undergo intense firearms training which qualifies them to carry weapons into the cockpit to protect themselves and their passengers. With few exceptions, these steps focused on denying the means to carrying out an attack. If airline security is to be truly effective, efforts must focus on screening out potential terrorists.

The Effects of 9/11 on the United States Economy

The effects of 9/11 on the U.S. economy were profound. One year after the disaster, it was clear that the attacks that rocked America also shook the world economy.[14] There were physical losses of more than $16 billion for U.S. businesses and the government, an additional $11 billion in rescue and clean up, and countless billions more for increased spending on public security in the United States, as well as in many other countries.[15] For the airline industry, the timing could not have been worse. Airports nationwide were closed for several days. Prior to the attacks, overall air travel and high-yield business flying were declining, with a forecasted loss of over $2.5 billion.[16] Immediately after September 11, airline traffic dropped 31 percent.[17] Although airplanes are normally a form of mass transportation, when they were cleared to operate, reluctant passengers refused to fly. This loss of vital revenue to a very cyclical but crucial sector of the economy was devastating to the airlines and increased downward pressure on U.S. markets. On 9/11, trading was halted on all U.S. exchanges. In the week after reopening, the New York Stock Exchange experienced its largest one-week (percentage point) drop in history. Equities lost $1.2 trillion in value. The yearly loss totaled $4 trillion.[18] Seventeen million Americans work in travel and tourist-related industries with an estimated payroll approaching $159 billion.[19] With so much revenue at stake in the travel industry and

with the markets reeling, easing the fear of travel that had gripped the nation since 9/11 took on strategic importance. Providing a more secure air transport system to further commerce became a necessity.

A Need for Change

While some of the changes made since 9/11 improved airline security, many of the requirements imposed provided more theatrics than real security. Too much emphasis was placed on the success of airlines at complying with Federal Aviation Regulations 107 (airport security) and 108 (aircraft operator security).[20] It is the amount of money an airline is fined annually by the FAA for security violations that has been used to benchmark success. Determining the best solution for revamping airline security is a complex exercise. There is not a single threat; there are multiple threats. Although Al-Qaeda remains the focus of the nation's attention, there are many extremists groups and sympathizers, criminals, copycats, and haters of the American way of life. To defend against this constant threat, airline security must remain a national-level concern. America must approach aviation security as a part of national defense. The Israelis have done just that. Surrounded by enemies and with their back to the sea, they have been pragmatic in their approach to preventing terrorist attacks on their airports. It has been more than thirty years since the last successful terrorist operation on El Al.[21] The U.S. security system is largely compliance-driven. In contrast, Israeli security is threat-driven. The American approach tries to screen out means. El Al focuses on screening out terrorists. This is not to say that Israelis are lax about keeping guns, knives, and bombs off of their jets. However, they place far greater emphasis on knowing who is getting on their jets than American does. The adoption of the Israeli's philosophy is essential if real air security in the United States is to be achieved. America must make use of the latest technological advancements.

The fielding of Transportation Workers Universal Identification Cards, fortress cockpit doors, body search x-ray equipment, and walk through "sniffer" devices would provide a significantly improved level of security. These advancements, when used in conjunction with better-trained and armed crews, would provide the in-depth defense needed. However, it is the use of biometrics that offers the greatest improvement available.

Biometrics

As previously stated, biometric systems consist of hardware and software used to capture various human characteristics and compare them to information stored in a database. Biometric identification is a three-step process. During the steps, a sensor makes an observation, the system describes the observation mathematically which produces a biometric signature, and the

computer inputs the biometric signature into a comparison algorithm and compares it to that in a database.[22] There are many biometric technologies available today. Fingertip recognition, hand geometry recognition, facial recognition, voice recognition, and iris/retinal recognition of some type are all in use in the United States. Fingertip recognition looks at the unique patterns found on fingertips and is considered highly accurate.[23] Facial recognition systems are also highly accurate. They measure the distance between a person's facial features, convert it into a code that a computer then uses to compare it with other face prints in a database.[24] The face recognition systems developed so far have not overcome the difficulties caused by variances in light, time of day, and the face angle when scanned.[25] Iris/Retinal recognition systems are eye-based systems that are generally considered to offer the best security.[26] Iris-based recognition uses the unique features found in the colored ring of tissue surrounding the pupil. Retinal recognition is probably the single most secure of all biometric systems. It uses the pattern of blood vessels at the back of the eye to determine identity.[27] Hand geometry recognition is a system that compares three-dimensional images of the fingers and knuckles to those stored in a database.[28] Voice recognition methods capture the sound of the speaker's voice then compare it to a prerecorded speech pattern.[29]

Identity management refers to the challenge of providing authorized users with secure and timely access to information and services across a variety of networked systems.[30] By recognizing individuals based on physiological characteristics, biometrics provides a natural (i.e. non-invasive) method of accurately determining identity.[31] This technology is already being tested at several airports in the United States to identify airport workers and frequent flyers. The goal of the program is to screen as many frequent fliers as possible, allowing those who pose little risk to move through quickly while giving screeners time to scrutinize others.[32] A relatively small pool of frequent fliers is responsible for more than half of the 774 million trips originating in the U.S. each year.[33] The ongoing tests involve several thousand frequent fliers and employees at major U.S. airports. Participants were required to submit names, addresses, phone numbers, dates of birth, and a biometric identifier. These data were then compared to that of intelligence and law enforcement officials. Palm and iris recognition devices have been placed at designated airport checkpoints to verify the identity of test participants, allowing selected passengers to bypass the long lines at the traditional screening lanes. Airport officials and travel associations are strongly advocating the use of biometrics in order to streamline passenger screening. "Improving the travel security experience will make travel more attractive, easier, and more efficient," said Michael Fogassey, Vice President of the National Business Travel Association's New England Chapter.[34] "We must provide strong, effective travel security

that does not hinder travel or place unnecessary burdens on the traveler," he said.[35] The concept has also been popular with members of Congress who fly frequently. [36]

Biometrics, used as a means of security, is not without its critics. John Daugman, who patented the idea in 1994, disputed the premise that the way to combat terrorism is to amass great quantities of data on individual citizens. "To confuse identification with antiterrorism is flawed reasoning," he said.[37] "It is an illusion to think iris scans could prevent terrorism."[38] If biometrics were to be used as a stand-alone security method, he, like many authorities on aviation security, has a valid point. A common concern among those opposing biometrics is that it will create a false sense of security. It is argued that a biometric system would provide too small of a benefit in return for the correlating significant loss of privacy. Others are disturbed at the idea of permitting some travelers to skip security steps such as removing shoes.[39] "Either making people take off their coat, shoes, and removing laptops has value or it doesn't," said Tim Sparapani, a privacy expert at the American Civil Liberties Union.[40] "If it does, then everyone should do it."[41]

Biometric systems are not invulnerable. Therefore, when deciding on a type of system, one must consider the ease by which it can be defeated. The four most important considerations are liveness, deception, data security, and physical space requirements.[42] Liveness refers to the ability of an intruder to trick face or voice recognition devices by using the picture, or recorded voice, of an authorized person.[43] Deception refers to methods such as the ability to lift then transpose fingerprints.[44] Data security refers to the interception of sensitive data being transferred and the use of it to defeat systems.[45] Physical space requirements refer to considerations that must be made based on where and how a system is installed.[46] Although seemingly vulnerable, the risks inherent in these biometric systems can be mitigated by using multiple types. Again, it is the use of multiple methods to screen and verify identity that provides the best security.

Impact of Change

Implementing change in the way airport security is conducted and justifying the cost inherent in a new strategy will not be easy. Americans tend to be reluctant to take on any additional financial burdens, despite knowledge that a more secure air travel industry will certainly be a benefit. The associated costs of a new system must be compared to the cost of doing nothing. Many of those who lost loved ones on September 11, 2001, can't imagine suffering such a loss again. Those surviving family members understand the necessity and impact of changes to the current security system. It is common knowledge that the fragile

airline industry, travel industry, and economy of the United States cannot afford another attack. The United States government, the airlines, and the traveling public must take the necessary steps to ensure that threats are identified. It will be the combined efforts of airlines, passengers, and the government that keep the industry free from the ever-present danger posed by terrorists.

The Transportation Security Administration has responsibility for aviation security procedures and must develop basic principles to guide the decision to employ threat-based biometric systems. These principles must be developed in coordination with federal, state, and local authorities. Civilian stakeholders, reviews of pertinent literature and data, and identification of best practices for implementing new programs must be considered. Foremost among these principles must be the rule that vulnerabilities in aviation security be assessed in a systematic way and addressed using a comprehensive risk management plan. The introduction of biometric-based security systems must be assessed in the broader context of border security and prioritized along with other programs designed to address security vulnerabilities. These programs include the security of ports and surface border crossings overseen by federal agencies such as the United States Department of Customs, the United States Coast Guard, and the Department of Immigration and Naturalization Services. The following principles should guide implementation:

- Apply lessons learned from existing programs. This information would include eligibility criteria, security procedures, and costs.
- Test the program to demonstrate its feasibility and effectiveness, and further validate the willingness of travelers to participate.
- Develop performance measures and a system for assessing how well the program meets stated mission goals.
- Select a system that can be easily updated to keep pace with new developments in security technology.
- Select a system that is interoperable with other access control points such as border crossings and ports of entry.[47]

When formulating strategy, it is often true that interests are at odds with each other. Such is the case with airline security. Careful consideration must be given to acceptability (minimum inconvenience), suitability (safe but mindful of civil liberties), and feasibility (cost). The cost of airline security prior to 9/11 was roughly $500 million per year. Today, such costs total nearly $3 billion per year.[48] Any plan designed to only allow access to cleared personnel while simultaneously providing the capabilities needed to defend against the infinite number of

weapons (and the means by which they can be brought on board) will be expensive and will infringe upon freedoms and liberties that Americans have previously considered sacred. The expenses incurred will include the costs of advanced screening devices, increased personnel salaries, interior and exterior modifications to airports, and the time and money required to conduct background investigations on airport employees. Considering the recent multiple bankruptcies filed by America's major carriers, these costs can only be borne by the citizen (i.e. increased fees for airline travelers or higher taxes for all Americans). Liberty infringements will be the disclosure of personal data and, when necessary, the submission to more detailed physical searches. This aspect, again, is a cost to the citizen. No one stand-alone system is capable of providing the security needs of a major airport. A sound security strategy must be based around the use of both technological advancements and the continued use of human screeners. Any successful method of securing airports will require that airport personnel and passengers be positively identified and continuously screened, and must include improved airport perimeter and interior security.

Shortly after the 9/11 attacks on the World Trade Center and the Pentagon, a screening of concession workers was conducted at Denver International Airport. The screening revealed the fact that many of the workers were illegal aliens. It will take the coordinated interagency efforts of local law enforcement, federal law enforcement, border patrol, immigration and naturalization services, national level intelligence agencies, and the synchronization of labors to mitigate the threat faced.

Many of the problems in security can be directly linked to the deregulation of air carriers in 1978. Upon deregulation, the government simply removed/eliminated many of the strict requirements under which airlines had previously been forced to operate. Essentially, deregulation allowed air carriers to forego passenger safety and security modernizations in order to maximize profit. As a result, today's airport security systems are not as technologically advanced as needed. In short, terrorists managed to defeat the rudimentary systems in place on 9/11 because they had been practicing on those same antiquated systems for years. Because of 9/11 and the recent attacks in London and Madrid, federal funding of transportation security has gained broad support in the U.S. Congress. Influential Senators Judd Gregg, Chuck Schumer, Richard Shelby, and Hillary Clinton are advocating increased spending in amounts ranging from $100 million to $1.3 billion.[49] William Millar, President of the American Public Transportation system, is seeking $6 billion.[50] However, prudence must be exercised while deciding which methods to fund. Homeland Security Secretary Michael Chertoff said, "The fact is that an airplane fully loaded with jet fuel, a commercial airliner, has the capacity to

kill 3,000 people. A bomb in a subway car may kill 30 people. When deciding priorities, you are going to think about making sure you don't have the catastrophic thing first."[51] In the past four years, the Department of Homeland Security has spent $250 million on transit security and $18 billion on aviation security, suggesting that these are ranked as they should be.[52] The role of the government in aviation security has increased. However, it is ironic that at the beginning of the 21st century there is a need to re-regulate parts of an industry that was recently deregulated.

Civil Liberties

Although the horrors of September 11, 2001, remain fresh in the minds of Americans, designing an improved and more in-depth air transport security system while simultaneously protecting the Constitutional (Fourth Amendment) rights will be challenging. The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[53]

Americans are accustomed to living in the most free and open society in the world. However, many citizens are beginning to feel that the Fourth Amendment rights are slowly disappearing. As a result of 9/11, security at American airports has been raised to the highest levels ever achieved. Entrance through security checkpoints is permitted only to those personnel in possession of a boarding pass. While curbside check-in has been reauthorized (after a temporary suspension), TSA employees now physically search 100% of checked luggage. Previously, such searches were done on a random basis and certain personnel, such as active duty military traveling on official government orders, were exempt. Complicating efforts to ensure all available technological advances are used to secure airport areas are rulings such as the pre-9/11 case, Kyllo vs. U.S., in which the Supreme Court held that the reasonable expectation of privacy could not be determined by the power of new technologies.[54] In what was considered a remarkable opinion written by conservative Justice Antonin Scalia, the court held that without a warrant, police could not use a new thermal imaging device that searches for heat sources to conduct what was the equivalent of a warrantless search in a home.[55] Although different in scope, this ruling emphasizes the determination of the highest court to uphold civil liberties and is an indicator of the challenges to be encountered with the implementation of any strategy that seemingly erodes freedoms. In the case of Chandler vs. Miller, the Court noted that "where the risk to public safety is substantial and real, blanket

suspicionless searches calibrated to the risk may rank as reasonable – for example, searches now routine at airports and at entrances to courts and other official buildings."[56] Organizations such as the American Civil Liberties Union, which filed claims against both airlines and airline security companies, are hindering security efforts. They claim that many of the techniques of "frisking personnel and conducting property searches," already in use at airports, are not only unconstitutional, but also in violation of civil liberties.[57] The question becomes one of "how much personal privacy is the traveling public willing to give up to achieve greater security?" The use of biometrics offers significant relief from profiling, frisking, and many of the other methods currently in use. Thanks to the immediate confirmation of identity (using the stored data) inherent with biometric scanning, only passengers not enrolled in the system and those who have somehow aroused "probable cause" would be subject to further screening.

A Strategy for Change

The President's National Security Strategy affirms the Nation's commitment to make the United States and the world a safer place.[58] The surest way to obstruct the development of a successful strategy for defending against attack is to let policy be guided by a series of knee-jerk reactions.[59] An airline security strategy must be adopted that best supports this commitment. Obviously, it is impossible to achieve 100% detection of potential weapons, since technological advances are used not only to build a better mousetrap but also to grow a better mouse. Twenty years ago, metal detectors were considered state-of-the-art security devices. No one carrying a handgun could pass through the detectors without triggering the alarm. The emergence of the Glock series of 9mm firearms (which are plastic, not metal, based) proved those supposedly "state-of-the-art" metal detectors were woefully inadequate. Technological advances are equally available to organizations on both sides of the ongoing war on terrorism. This is the underlying reason that a new strategy must be threat-based, as opposed to means-based, recognizing the true dimensions of the threat. There is no single threat; rather, there are multiple threats. As clearly explained above, the United States must move away from the means-based strategy currently in use. America must positively identity all passengers traveling on jets. The attacker always has the advantage of choosing where to attack, and terrorists look for weaknesses in defenses just as Hitler's army sidestepped the Maginot Line.[60.] Successful strategists have always taken advantage of their enemy's vulnerabilities, attacking through the area that had the weakest defense. Such has been the strategy of winning armies since the time of Henri Jomini during the French Revolution. As discussed during the United States Army War College staff ride, the Battle of Gettysburg was doomed to fail because General Robert E.

Lee insisted on waging a full frontal attack, much to the dismay of his senior advisery staff. Lee did not pursue the path of least resistance, as do the terrorists of today.

The following airline security objectives are proposed:

- Safeguard the national and international air transport system from attack
- Ensure strategic access to national and international airspace
- Partner with other nations to ensure the most up to date security systems are in place
- Avoid needless infringements upon civil liberties

The methods employed to achieve these strategic objectives should be based on the use of biometric systems in conjunction with the more traditional methods currently used by the Transportation Security Administration to positively identify everyone entering secure airport areas. To recap, current methods include physical body searches conducted by TSA employees, metal detectors through which passengers must walk, hand-searches of checked baggage, and x-ray screening of carry-on items. Americans must never forget that a poorly conceived strategy is expensive, a bad strategy can be lethal, and a very bad strategy is almost always fatal.[61]

Assessing Risk

Risk management is the foundation of any successful strategy. The approach to good security is fundamentally similar regardless of the asset being protected. There are five questions whose answers must be thoroughly understood if practical and cost-effective security is to be achieved.

- What is being protected? The asset being protected must be identified and the impact of its loss determined.
- Who is the adversary? Know the intent and capability of the threat.
- What are the vulnerabilities? Identify vulnerabilities and weaknesses that would allow the threat to be realized.
- What are the priorities? Assess the level of risk and determine priorities. Determine the impact of loss or damage to the asset, threats to the asset, and vulnerabilities.
- What can be done? Compare advantages of proposed actions to disadvantages to determine how best to mitigate risk.[62]

Prior to adopting a new strategy, both a comprehensive cost-benefit analysis and a thorough risk-benefit analysis must be completed. When trying to establish an acceptable amount of risk, societal values, the safety of aircrews and passengers, and the costs inherent in any recommendation must be considered. Ends, ways, and means will have to be carefully

balanced in an effort to arrive at the most effective and efficient method of securing the skies. The desired end state is known. Americans want an airport security system that allows the safe conduct of air commerce with minimum inconvenience to the traveler. With five of the nation's ten largest airlines (United, Delta, Northwest, America Trans Air, and US Air) in bankruptcy, the means will, out of necessity, be the responsibility of the government. It is the ways that will be most difficult to determine. America was formed as a free and open society. Any decision that erodes the ability to travel freely, or enables one to do so only with restrictions or intense security screening, must be carefully analyzed. A determination must be made with the knowledge that "we don't know what we don't know" about how a very determined threat will attack next. Because of the very nature of the threat faced, the best decision possible with limited information must be made.

> Defending our nation against its enemies is the first and fundamental commitment of the federal government. Today, that task has changed dramatically. Enemies in the past needed great armies and great industrial capabilities to endanger America. Now, shadowy networks of individuals can bring great chaos and suffering to our shores for less than it costs to purchase a single tank.
>
> —President George W. Bush, September 2002.[63]

Conclusion

Anyone working within the air transport system is painfully aware of the tremendous problem that providing adequate security poses and of the associated strategic ramifications. Air transport workers certainly do not have all of the answers and have not pretended to know the best strategy; however, they agree that there must be a strategy. The chosen strategy must be one that is palatable, both domestically and abroad. The safe and secure conduct of air commerce is of national and international importance. The fact that the airline industry serves as a form of mass transportation tempts one to believe that the income and profit derived from passengers flying domestic routes constitutes the bulk of the airlines' revenue, making it the most valuable impact airlines provide to the nation's economy. Contrary to that misconception, it is the transport of international freight, followed by the income obtained from corporate travelers, both domestic and international, that generates the most revenue. The maintenance of a secure air transport system is, therefore, a matter of international economic concern.

The events of September 11, 2001, had a profound effect on the United States and caused defense of the Homeland and the air transport system to be the 21st century's first major challenge. Much has been done to provide the defenses needed to secure the skies while simultaneously protecting American's civil liberties. Changes in airport design, new methods of

securing aircraft, a greater awareness by travelers, and the arming of pilots have combined to create a more secure industry. However, the multiple threats directed against America require constant vigilance and a dynamic approach to airline security that is forward looking and visionary. It is clear that the method by which defense against terrorism must be continuously evaluated with a focus toward defeating a determined adversary. Only through continued exploration and the exploitation of cutting-edge technology, can the necessary in-depth defense be provided. Nay-sayers will argue that the loss of privacy inherent in providing so much information to computer systems constitutes too high a price to pay for the benefit that is gained; in essence, the ends do not justify the means. Conversely, supporters will argue that the use of such technologically advanced biometric identification systems, coupled with the expedience at which screening will take place, create a benefit that far outweighs the corresponding loss of some privacy. Regardless of the aforementioned (and highly controversial) issue of potential civil rights violations, research indicates that the widespread use of biometric scanning and identification systems will unquestionably provide a vast improvement in air transport security. "Freedom isn't free." If the citizens of the United States want to continue to enjoy the much-cherished openness of modern transportation systems, they must be willing to sacrifice some of those rights that allowed the tragedy of September 11, 2001, to occur.

Endnotes

[1] George W. Bush, "Executive Order Establishing Office of Homeland Security," *Executive Order,* available from http://www.whitehouse.gov/news/releases/2001/10/20011008-2.htm; Internet; accessed 1 November 2005.

[2] Mimi Hall, "Ex-official tells of Homeland Security Failures," *USA Today,* 28 December 2004; available from http://www.usatoday.com/news/washinton/2004-12-27-homeland-usat_x.htm; Internet; accessed 1 November 2005.

[3] David Krajicek, "D.B. Cooper: The Legendary Daredevil," *The Hijacking Dilemma;* available from http://www.crimelibrary.com/criminal_mind/scams/DB_Cooper/3.html; Internet; accessed 1 November 2005.

[4] Fatal U.S. Hijacking Events Since 1970, *Airsafe.com News*, available from http://www.airsafe.com/events/hijack.htm; Internet; accessed 20 October 2005.

[5] George W. Bush, "Governor Ridge Sworn–In to Lead Homeland Security," speech, The White House, Washington, D.C. October 8, 2001.

[6] Deneen Brown, "International Flights Diverted to Canada," *The Washington Post,* 12 September 2001, E.06.

[7] Michael A. Canavan, “Terrorist Attacks Upon the United States,” speech, National Commission on Terrorist Attacks Upon the United States, 23 May 2004, available from http://www.9-11.commission.goc/hearings/hearings2/witnesscanavan.htm; Internet; accessed 5 November 2005.

[8] Office of Homeland Security, The National Strategy for Homeland Security, 2 July 2002, iii

[9] Ibid, p vii

[10] TSA Fact Sheet – September 11, 2003, available from http://www.tsa.gov/public/display?heme=44&content=09000519800502ce; Internet; accessed 1 November 2005.

[11] Ibid.

[12] U.S. Congress, Committee on Transportation and Infrastructure, Subcommittee on Aviation, Hearing on Status of the Federal Flight Deck Officer Program, 23 January 2002.

[13] Michael Loh, “FAA: A Failure on Aviation Security,” *Aviation Week & Space Technology*, New York: 8 October 2001. Issue 15 p 94.

[14] Rana Foroohar, “A Blow to Global Trade; The economic impact of the attacks is becoming clear,” *Newsweek (International ed.),* New York: 9 September 2002. 44

[15] Ibid.

[16] Stanley Holmes and Stan Crock, *Business Week,* New York: 14 January 2002, Issue 3765 p 90.

[17] Cindy Loose and Gary Lee, “A Year Later, the Travel World is Still Spinning,” *The Washington Post,* 8 September 2002. p. E.05.

[18] Michael Treis, “Economic Aftermath–Follow the money!” *Wikipedia,* 14 April 2005, available from http://en.wikipedia.org/wiki/September_11 ,_2001_attacks; Internet; accessed 2 November 2005.

[19] Bill Powell, “The Economy Under Siege,” *Fortune Magazine,* 15 October 2001. 90.

[20] Federal Aviation Administration “FAR Parts 107 and 108,” Federal Aviation Regulations, available from http://www.flightsimaviation.com/data/FARS/PART107.html; Internet; accessed 5 November 2005.

[21] “El Al Sets Security Standards,” BBC News, 5 July 2002, available from http://news.bbc.co.uk/1/hi/world/americas/2097352.stm; Internet; accessed 1 November 2005.

[22] Ravi Das, “An Introduction to Biometrics,” *Military Technology,* 29 July 2005. Military Module, 21

[23] Ibid., 22.

[24] Ibid., 23.

[25] Fred Guterl, “Taking A Closer Look,” *Newsweek (International ed.),* 8 March 2004, 42.

[26] Das, 24.

[27] Ibid.

[28] Ibid.

[29] Das, 25.

[30] Nandakumar Karthik, *Integration of Multiple Cues in Biometric Systems*, Graduate Thesis, (Michigan State University, 2005). available from http://biometrics.cse.msu.edu/Karthik_thesis05.pdf; Internet; accessed 2 November 2005.

[31] Ibid.

[32] Laura Meckler, "Air Security: Shorter Waits For More Fliers?" *Wall Street Journal,* 28 September 2005 B.1; available from ProQuest; accessed 1 November 2005.

[33] Ibid.

[34] "Registered Traveler Launches at Boston Logan," *Airports,* 24 August 2004, Vol.21, issue 34 p 3.

[35] Ibid., 4.

[36] Sara Goo, "Registered Traveler Test Ends Inconclusively; Airport Security Scheme Lacks Broad Support," *The Washington Post,* 27 September 2005, p. A.15

[37] Guterl.

[38] Ibid.

[39] Meckler.

[40] Ibid.

[41] Ibid.

[42] Das, 26.

[43] Ibid.

[44] Ibid.

[45] Ibid.

[46] Das, 27.,

[47] United States General Accounting Office, "Registered Traveler Program Policy and Implementation Issues," *Aviation Security* Report to the Honorable Kay Bailey Hutchinson, U.S. Senate, November 2002.

[48] "The Cost of Airline Security," The Travel Insider, 30 April 2004, available from http://thetravelinsider.info/2004/email0430.htm; accessed 6 November 2005.

[49] Veronique Rugy, "The Right Fight – Put Security Dollars Where It Counts," *National Review,* 29 August 2005, available from http://m01.webmail.aol.com/display-message.aspx; Internet; accessed 2 November 2005.

[50] Ibid.

[51] Ibid.

[52] Ibid.

[53] Jay Stanley and Barry Steinhardt, "Bigger Monster, Weaker Chains: The Growth of an Amerian Surveillance Society," *ACLU Technology and Liberty Program* , 15 January 2003, available from http://www.ratical.org/ratville/CAH/BWWC.html; Internet; accessed 2 November 2005.

[54] Ibid.

[55] Ibid.

[56] Sherry Colb, "Breast Exams at the Airport," *Find Law's Legal Commentary,* 1 December 2004.

[57] Samantha Murphy, "ACLU: Airport Frisks Are Invitation To Sexual Harassment," Court TV, 23 November 2004, available from http://www.cnn.com/2004/LAW/11/23/airport.security/ ; Internet; accessed 2 November 2005.

[58] Richard B. Meyers, *National Military Strategy of the United States of America 2004* (Washington, D.C. The Pentagon, 2004), iii.

[59] Rugby.

[60] Ibid.

[61] Colin S. Gray, *Modern Strategy:* (Oxford University Press, 1999), 1.

[62] Keith Rhodes, "Challenges in Using Biometric Technologies," *Aviation Security*, Testimony Before the Subcommittee on Aviation, Committee on Transportation and Infrastructure, House of Representatives, May 2004.

[63] George W. Bush, *National Security Strategy of the United States of America 2002 (Washington, D.C. The Pentagon, 2004), iii.*

[64] Warren Villareal, Captain, United Airlines, telephone interview by author 13 November 2005. Synthesis of thoughts must be partially attributed to this airline security expert.

[65] Ed Folson, Captain, United Airlines, telephone interview by author 18 June 2005. Synthesis of thoughts must be partially attributed to this airline security expert.